Dynamic Reliability Modeling of Cooperating Digital-Based Systems

Florent Brissaud, Carol Smidts, Anne Barros, Christophe Bérenguer

Dynamic Reliability Modeling of Cooperating Digital-Based Systems

F. Brissaud
Institut National de l'Environnement Industriel et des Risques (INERIS), Verneuil-en-Halatte, France
Université de Technologie de Troyes (UTT) – Institut Charles Delaunay (ICD) & UMR CNRS 6279 STMR, Troyes, France

C. Smidts
Ohio State University (OSU), Columbus, USA

A. Barros & C. Bérenguer
Université de Technologie de Troyes (UTT) – Institut Charles Delaunay (ICD) & UMR CNRS 6279 STMR, Troyes, France

ABSTRACT: Dynamic reliability explicitly handles the interactions between the stochastic behavior of system components and the deterministic behavior of process variables. However, its industrial level applications are still limited, notably due to the inherent complexity of the theory and the lack of a generic modeling framework. The increased use of digital-based systems has also introduced additional modeling challenges related to the interactions between cooperating digital components. For solving these challenges, the present paper first extends the mathematical framework of dynamic reliability to handle 1) information and data computed and exchanged between digital components; and 2) random parameter deviations. A formalized Petri net approach is then proposed to perform the corresponding reliability analyses, using a finite element method. Finally, the framework's effectiveness is demonstrated on a simplified model of a nuclear reactor case study.

1 INTRODUCTION

Probabilistic risk (or safety) assessments (PRA) provide a general framework for managing risks linked to engineering systems, notably in nuclear power plants, aerospace, and chemical industries. The main purpose of PRA is to identify the possible accidental scenarios, to rate their consequences, and to assess their likelihoods. An essential challenge is to deal with the system complexity, that is, to treat system interactions both efficiently and realistically.

In the seventies, the event tree/fault tree methodology was introduced for PRA (US NRC 1975), focusing on system components and their "static" relationships. In the late eighties-early nineties, dynamic reliability (or probabilistic dynamics) methods were developed to explicitly handle the influence of time, process dynamics and human operations, on system failures and PRA scenarios. These approaches include dynamic discrete-time event trees (e.g. DYLAM, DETAM), the GO-FLOW methodology, Event Sequence Diagrams (ESD), the Dynamic Flowgraph Methodology (DFM), Markov models, and Petri Nets. Most of them have been presented, compared and discussed by Aldemir *et al.* (1994), Siu (1994), and Labeau *et al.* (2000). Although there is a broad consensus on the need for dynamic reliability methods (Aldemir & Siu 1996), such approaches have not yet penetrated the arena of industrial applications (Labeau *et al.* 2000). Given reasons are the theoretical flavor and the lack of a generic platform for performing such analyses.

The formal mathematical framework of dynamic reliability was established under the name of Continuous Event Tree (CET) theory, (Devooght & Smidts 1992a). The latter introduced two sets of variables to define the complete system state:

– physical (continuous) variables of the process (e.g. level, pressure, temperature);
– state (discrete) variables of the system components (i.e. system configuration).

The evolution of the process variables was characterized by a set of first order (non-stochastic) differential equations for each value of state variables. Changes in state variables were assumed stochastic, defined by transition rates, and dependent on process variables. Human operations were also included as additional variables (Devooght & Smidts 1992b).

More recently, the use of digital safety-related systems has introduced new issues for dynamic reliability modeling, especially due to the interactions between system components (Aldemir et *al.* 2006). Typical examples of such systems include the "intelligent transmitters" which are able to exchange information, to perform internal data processing and advanced functionalities (Brissaud *et al.*, sub.).

The present paper focuses on the dynamic reliability modeling of cooperating digital-based systems. First, the mathematical framework of dynamic reliability is extended in Section 2 to deal with the specific characteristics of these systems. A formalized Petri-net approach is also proposed to perform the related reliability analyses. Finally, a case study involving a nuclear reactor is presented in Section 3.

2 DYNAMIC RELIABILITY FRAMEWORK FOR COOPERATING DIGITAL-BASED SYSTEMS

2.1 *Problem Formulation*

In addition to time t, four types of variables are used to describe the complete system state. The process and components state variables remain the same as those defined by Devooght & Smidts (1992a). Data variables are introduced in order to characterize digital systems; and deviation variables extend the possibilities of failure modeling. All these variables are time-dependent. The process, data, and deviation variables are continuous and depicted by vectors of reals, respectively denoted $\boldsymbol{x(t)}$, $\boldsymbol{y(t)}$, and $\boldsymbol{e(t)}$. Components state variables are discrete and depicted by a vector of integers, denoted $\boldsymbol{i(t)}$. (cf. Table 1).

The process variables $\boldsymbol{x(t)}$ represent the physical variables involved in the system dynamics (e.g. pressure, temperature, volume). They evolve deterministically, given components state, and with deviations as parameters (e.g. the level in a tank is determined by the configuration of the valves, and the amount of leakage). The evolution of process variables may then usually be defined by a set of first order differential equations, indexed by the components state:

$$\frac{d}{dt}\boldsymbol{x(t)} = \boldsymbol{x'_i(x, e, t)} \tag{1}$$

The data variables $\boldsymbol{y(t)}$ represent any information or data which are computed, stored, and/or exchanged between system components (e.g. commands, measurement results, diagnostic information). By nature, they do not directly affect process and deviation variables, but are used to change components state. The data variables may usually be expressed as a function of process and deviation variables, given components state (e.g. when a transmitter is in a non-fully operating mode i.e. a component state, its measurement results depend on the quantities to be measured i.e. process variables, and drifts i.e. deviation variables). The data variables may also depend on their previous values (e.g. stored data, locked signals), denoted $\bar{}\boldsymbol{y(t)}$, with $\bar{}\boldsymbol{y(t)} = \boldsymbol{y(t - \varepsilon)}$ and ε which tends to 0^+:

$$\boldsymbol{y(t)} = \boldsymbol{y_i(x, \bar{}y, e, t)} \tag{2}$$

The deviation variables $\boldsymbol{e(t)}$ represent continuous errors or deviations in system properties, which evolve stochastically (e.g. system degradations, drifts), depending on process variables and components state (e.g. the leak in a closed valve follows a random distribution influenced by the flow rate). Because the evolution of deviation variables is continuous, it may usually be defined by a set of first order differential equations which include random variables (e.g. the rate of crack growth is a random variable which depends on the current crack level), indexed by the components states:

Table 1. Nomenclature

Variable	Description
t	time
$\boldsymbol{x(t)}$	vector of process variables at time t
$\boldsymbol{y(t)}$	vector of data variables at time t
$\bar{}\boldsymbol{y(t)}$	vector of previous values of $\boldsymbol{y(t)}$ up to time t
$\boldsymbol{e(t)}$	vector of deviation variables at time t
$\boldsymbol{i(t)}$	vector of components state variables at time t
$\boldsymbol{x'_i(x, e, t)}$	expression of derivatives of process variables at time t, given $\boldsymbol{i(t)}$, $\boldsymbol{x(t)}$, and $\boldsymbol{e(t)}$
$\boldsymbol{y_i(x, \bar{}y, e, t)}$	expression of data variables at time t, given $\boldsymbol{i(t)}$, $\boldsymbol{x(t)}$, $\bar{}\boldsymbol{y(t)}$, and $\boldsymbol{e(t)}$
$\boldsymbol{E'_i(x, e, t)}$	vector of random variable which provides the rate of change of deviation variables at time t, given $\boldsymbol{i(t)}$, $\boldsymbol{x(t)}$, and $\boldsymbol{e(t)}$
$\boldsymbol{i}^k$	specific value of vector $\boldsymbol{i(t)}$, indexed by k
$p(\boldsymbol{i}^k \to \boldsymbol{i}^l \mid \boldsymbol{x,y,e,t})$	components transition rate from state $\boldsymbol{i}^k$ to state $\boldsymbol{i}^l$ at time t, given $\boldsymbol{x(t)}$, $\boldsymbol{y(t)}$, and $\boldsymbol{e(t)}$
$\lambda_{ik}(\boldsymbol{x, y, e}, t)$	total components transition rate from state $\boldsymbol{i}^k$ at time t, given $\boldsymbol{x(t)}$, $\boldsymbol{y(t)}$, and $\boldsymbol{e(t)}$
$F_{ik}(\tau \mid \boldsymbol{x, y, e}, t)$	probability of leaving components state $\boldsymbol{i}^k$ in time interval $[t, t + \tau[$
$\boldsymbol{P_i(x, y, e}, t)^T \cdot \boldsymbol{\ddot{I}}$	product of vectors which determine randomly $\boldsymbol{i(t+\Delta t)}$ according to transition rates
$\boldsymbol{(i, x, y, e}, t)$	notation for $\boldsymbol{(i(t), x(t), y(t), e(t))}$, description of the complete system state at time t
Δt	time step

$$\frac{d}{dt}\boldsymbol{e(t)} = \boldsymbol{E'_i(x, e, t)} \tag{3}$$

where $\boldsymbol{E'_i(x, e, t)}$ is a (function of) random variable.

The components state variables $\boldsymbol{i(t)}$ represent the structure (configuration) of the system and is a function of the states of its components (operating or failed) and of human operations (e.g. opening or closing a valve). The state of any system component (e.g. operational, degraded, or failed) can be described by integers which are arranged in vector $\boldsymbol{i(t)}$. The components state variables may evolve both deterministically and stochastically, depending on process and data variables (e.g. a valve is controlled by a signal; a transmitter failure rate depends on the temperature), and deviations (e.g. after a certain level of degradation, a component transition occurs from a degraded mode into a fully non-operating mode). The components transition rate from state $\boldsymbol{i}^k$ to state $\boldsymbol{i}^l$ at time t, given process, data, and deviation variables, is denoted $p(\boldsymbol{i}^k \to \boldsymbol{i}^l \mid \boldsymbol{x, y, e}, t)$. Then, the total components transition rate from state $\boldsymbol{i}^k$ is:

$$\lambda_{ik}(\boldsymbol{x, y, e}, t) = \sum_{i^l \neq i^k} p(\boldsymbol{i}^k \to \boldsymbol{i}^l \mid \boldsymbol{x, y, e}, t) \tag{4}$$

The transitions between components states are assumed instantaneous. When the components state at time t is $\boldsymbol{i(t)} = \boldsymbol{i}^k$, the probability that the components leave this state before time $t + \tau$ is therefore:

$$F_{ik}(\tau \mid \boldsymbol{x,y,e},t) = 1 - \exp\left(-\int_0^{\tau} \lambda_{ik}(\boldsymbol{x,y,e},t+u)\cdot du \right) \tag{5}$$

2.2 *Mathematical Solution Using a Finite Element Method*

For the numerical analyses of the complete system evolution according to time, a finite element method is adopted. A time step Δt is used which should be small enough to assume that variables $\boldsymbol{x(t)}$, $\boldsymbol{y(t)}$, $\boldsymbol{e(t)}$, and $\boldsymbol{i(t)}$ are constant in any time interval $[t, t + \Delta t[$ without loss of accuracy. These variables at time $t + \Delta t$ can then be determined by their values at time t. In particular, a components state transition which occurs between time t and time $t + \Delta t$ is considered to occur exactly at time $t + \Delta t$. In the same way, the evolution of the process, data, and deviation variables between time t and time $t + \Delta t$ are considered to occur as "jumps" exactly at time $t + \Delta t$. It is then possible to approximate the values of process and deviation variables at time $t + \Delta t$, according to the complete system state at time t, using the finite differences of the derivatives given in Section 2.1:

$$\boldsymbol{x}(t + \Delta t) \approx \boldsymbol{x}(t) + \Delta t \cdot \boldsymbol{x'_i}(\boldsymbol{x}, \boldsymbol{e}, t) \quad (6)$$

$$\boldsymbol{e}(t + \Delta t) \approx \boldsymbol{e}(t) + \Delta t \cdot \boldsymbol{E'_i}(\boldsymbol{x}, \boldsymbol{e}, t) \quad (7)$$

In addition, the probability that the components remain in their current state at time t, denoted $\boldsymbol{i}(t) = \boldsymbol{i}^k$, up to time $t + \Delta t$, that is $\boldsymbol{i}(t + \Delta t) = \boldsymbol{i}^k$, is:

$$\Pr[\boldsymbol{i}(t + \Delta t) = \boldsymbol{i}^k \mid \boldsymbol{i}(t) = \boldsymbol{i}^k, \boldsymbol{x}, \boldsymbol{y}, \boldsymbol{e}, t]$$
$$= 1 - F_{ik}(\Delta t \mid \boldsymbol{x}, \boldsymbol{y}, \boldsymbol{e}, t) \approx 1 - \Delta t \cdot \lambda_{ik}(\boldsymbol{x}, \boldsymbol{y}, \boldsymbol{e}, t) \quad (8)$$

And similarly, the probability that the components leave their current state at time t, denoted $\boldsymbol{i}(t) = \boldsymbol{i}^k$, for another specific state at time $t + \Delta t$, denoted $\boldsymbol{i}(t + \Delta t) = \boldsymbol{i}^l$, with $\boldsymbol{i}^k \neq \boldsymbol{i}^l$, can be approximated by:

$$\Pr[\boldsymbol{i}(t + \Delta t) = \boldsymbol{i}^l \neq \boldsymbol{i}^k \mid \boldsymbol{i}(t) = \boldsymbol{i}^k, \boldsymbol{x}, \boldsymbol{y}, \boldsymbol{e}, t]$$
$$\approx \Delta t \cdot p(\boldsymbol{i}^k \rightarrow \boldsymbol{i}^l \mid \boldsymbol{x}, \boldsymbol{y}, \boldsymbol{e}, t) \quad (9)$$

Note that a deterministic (certain) transition can then be modeled using a rate equal to $1/\Delta t$.

The couple $(\ddot{\boldsymbol{I}}, \boldsymbol{P_i}(\boldsymbol{x}, \boldsymbol{y}, \boldsymbol{e}, t))$ is defined, with $\ddot{\boldsymbol{I}}$ a vector composed of all possible combinations of components states, and $\boldsymbol{P_i}(\boldsymbol{x}, \boldsymbol{y}, \boldsymbol{e}, t)$ a vector with all its components equal to 0 except one that is equal to 1 whose components are determined randomly according to Equations (8) and (9), in such a way that:

$$\boldsymbol{i}(t + \Delta t) \approx \boldsymbol{P_i}(\boldsymbol{x}, \boldsymbol{y}, \boldsymbol{e}, t)^T \cdot \ddot{\boldsymbol{I}} \quad (10)$$

Once the components state, process and deviation variables are defined at time $t + \Delta t$, the data variables at time $t + \Delta t$ can also be determined, using $\varepsilon = \Delta t$ which implies that $\bar{\boldsymbol{y}}(t + \Delta t) = \boldsymbol{y}(t)$:

$$\boldsymbol{y}(t + \Delta t) \approx \boldsymbol{y_i}(\boldsymbol{x}, \bar{\boldsymbol{y}}, \boldsymbol{e}, t + \Delta t) \quad (11)$$

Equations (6)-(11) show that the complete state of the system at time $t + \Delta t$, i.e. $(\boldsymbol{i}, \boldsymbol{x}, \boldsymbol{y}, \boldsymbol{e}, t + \Delta t)$, can be fully determined according to its state at time t, i.e. $(\boldsymbol{i}, \boldsymbol{x}, \boldsymbol{y}, \boldsymbol{e}, t)$, according to deterministic and stochastic evolutions. The system is therefore a piecewise-deterministic process (PDP), (Davis 1993).

2.3 *Petri Net Formalism for Numerical Analyses*

Petri nets and their extensions, including stochastic and colored characteristics, provide natural and effective tools for modeling dynamic systems (David & Alla 1994), notably for risk analysis (Vernez *et al.* 2003). Stochastic Petri nets were also used efficiently in dynamic reliability (Dutuit *et al.* 1997). In the present paper, a Petri net formalism, using stochastic and colored properties, is proposed in order to provide a generic framework to:

- flexibly model the dynamic reliability of a system with the help of a visual interface easy to handle;
- simulate the evolution of the complete system state, using a finite element method.

In the proposed approach, each place of the Petri net is associated to one set of variables, and vice-versa. The number of places then increases linearly according to the number of variables, which avoids any combinatorial explosion. According to the nature of the variables (continuous or discrete, stochastic or deterministic), different representations are used for graphical convenience (cf. Figure 1). The values of the variables are given by the (colored) token, with real or integer numbers (according to the places) inside the corresponding places, and are changed by the transitions. Each place therefore always contains one and only one token, and thus, all the transitions are always enabled. Guards are then used for each transition and denoted $s_j[\Delta t]$, which means that the transition is fired at each time instant $s_j + k \cdot \Delta t$, with $k = 0, 1, 2, \ldots$

Each transition of the Petri net is associated to a place, denoted "managed place." This place is linked to the transition by an input arc, which means that the corresponding variables are changed by the transition ("the token is removed from the place"); and linked to the same transition by an output arc, which attributes to the variables their new values ("the token is deposited in the place"). An expression is given on this output arc to specify these new values, which may depend on the previous values of the variables (handled by the input arc) and also on variables from other places. The latter places are then denoted "dependence places" and are linked to the corresponding transition by bi-directed arcs, which means that the values of their variables may be used by the transition, but are not changed.

The new values of variables (specified by the output arcs from the transitions to their "managed places") may also depend on random variables. Contrarily to the "classical" stochastic Petri nets, the stochastic aspects therefore do not relate to time instants, but to values of variables (i.e. the token "color"). In this approach, the time, as a variable, is modeled by a place. Besides, all the transitions are fired at deterministic time instants (specified by the transition guards). This approach can therefore be classified as an "untimed stochastic (and colored) Petri net."

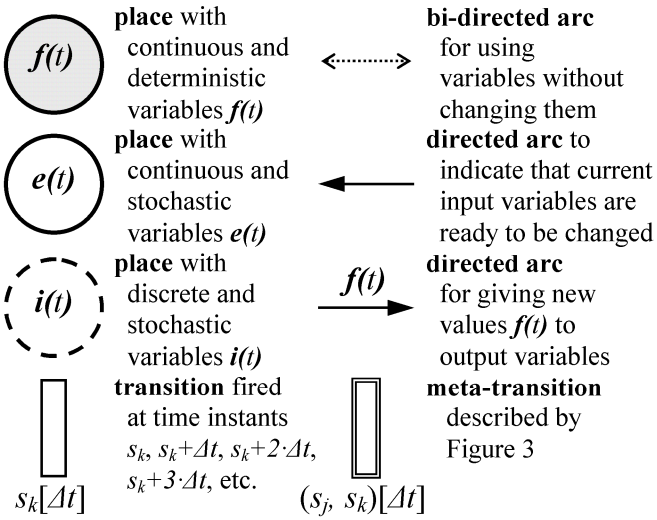

Figure 1. Petri net tool box.

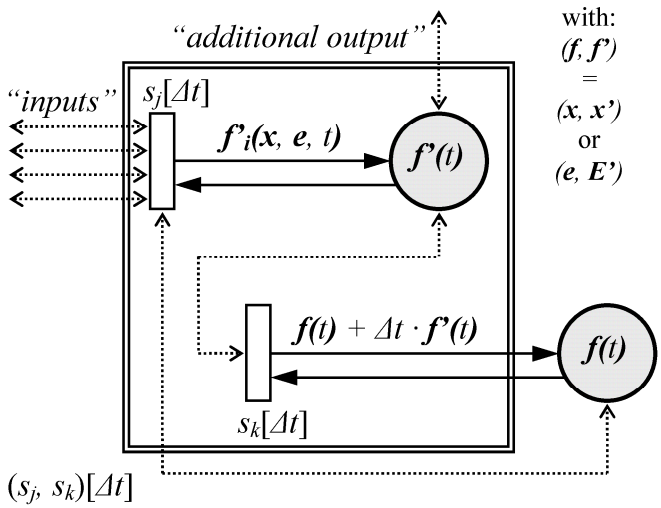

Figure 3. Meta-transition for Petri net.

A generic Petri net for the dynamic reliability modeling of systems is depicted in Figure 2, using the elements described in Figure 1. The five types of variables defined in Section 2.1 are modeled, and depicted using different varieties of places. In Figure 2, the variables are represented by vectors (except for time t). For more detailed models, it is also possible to split these vectors into subsets with one place for each (subset), and to treat them separately.

Each transition is fired at every time step Δt, changing the variables modeled by the corresponding "managed place," according to the equations given in Section 2.2 and specified on the output arcs. The transition that changes the time variable t is not linked to any "dependence place" and is simply used to increment time t by Δt at each solicitation. On the other hand, the components state variables $\boldsymbol{i(t)}$ are changed by random variables defined by Equation (10), which depend on all the variables.

In each time interval $[t, t + \Delta t]$, all the values of variables at time $t + \Delta t$ are computed following a specific order defined by the s_j (cf. top of Figure 2). (Such specific orders may also be required to deal with dependencies between subsets of variables.) Note that the values of variables at time $t + \Delta t$ depend on values at time t (cf. Equations (6)-(11)). In particular, $\boldsymbol{x}(t + \Delta t)$ and $\boldsymbol{e}(t + \Delta t)$ both depend on $\boldsymbol{x}(t)$ and $\boldsymbol{e}(t)$. To avoid "losing" the values of $\boldsymbol{x}(t)$ (resp. $\boldsymbol{e}(t)$) after computing $\boldsymbol{x}(t + \Delta t)$ (resp. $\boldsymbol{e}(t + \Delta t)$), "Meta-transitions" are introduced. They are used to first compute all the derivatives at time t (i.e. $\boldsymbol{x'_i(x, e, t)}$ and $\boldsymbol{E'_i(x, e, t)}$), storing them as additional variables (cf. Figure 3), and then to change the variables of the complete system state. A "Meta-transition" has therefore a double guard denoted $(s_j, s_k)[\Delta t]$, which means that the derivative is computed at each time instant $s_j + k \cdot \Delta t$, and the variables of the "managed place" at $s_k + k \cdot \Delta t$.

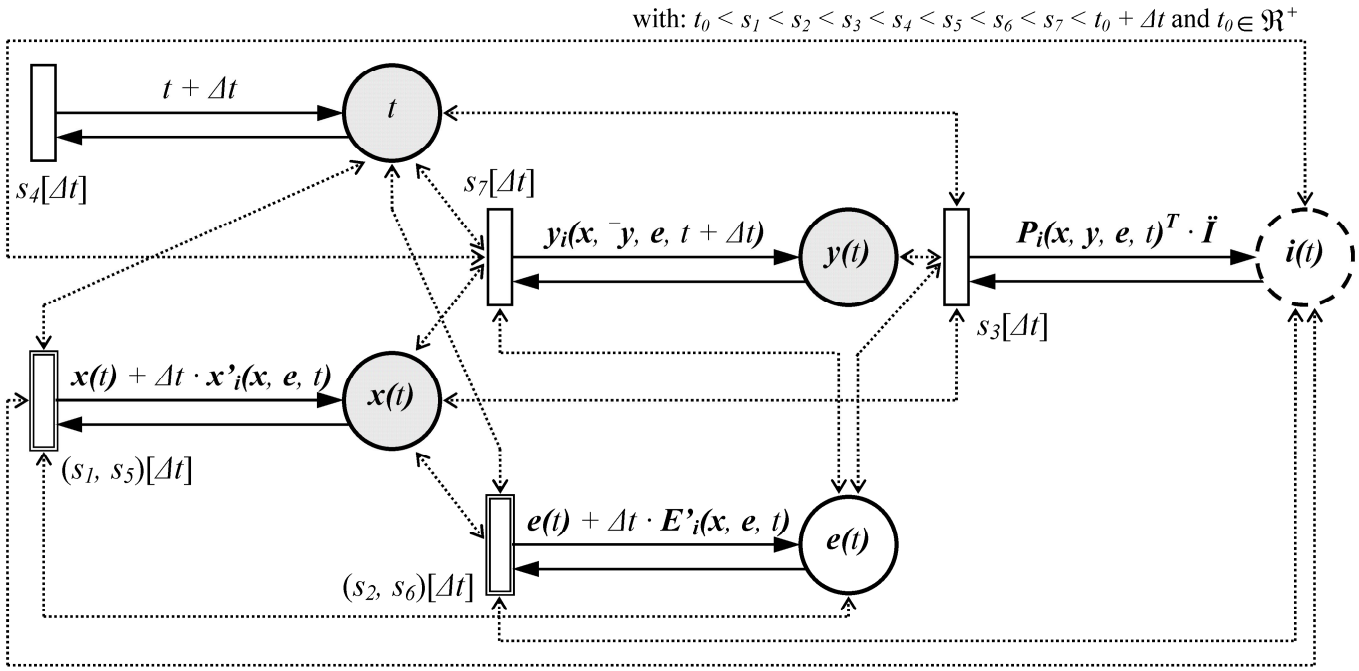

Figure 2. Generic Petri net for the dynamic reliability modeling of systems.

3 CASE STUDY OF A FAST REACTOR

3.1 *The Europa Fast Reactor*

The case study is the primary circuit of the Europa fast reactor. This system has been proposed as a benchmark problem on accident sequences (Wider *et al.* 1989). Several dynamic reliability analyses have been also performed on this application (Amendola & Reina 1984, Smidts & Devooght 1992, Swaminathan & Smidts 2000). A comprehensive description of the system is provided by Smidts & Devooght (1992). In the present paper, the physical variables have been simplified to allow us to focus more specifically on other aspects. In particular, new transmitter features have been introduced (communications and drift corrections), and deviation variables.

The simplified model of the primary circuit of the Europa fast reactor is depicted in Figure 4. This system is comprised of two channels (C1 and C2) where sodium is introduced as a coolant by a pump (PM). The lack of coolant, for example in case of a pump failure, increases the temperature in the channels and may yield hazardous events. The sodium temperatures in the channels (T_1 and T_2) are therefore monitored by transmitters (ST1 and ST2) which send their results ($T1^s$ and $T2^s$) to a common controller (CT). Similarly, the flow rate (G) is monitored by a third transmitter (SG) which sends its result (G^s) to another controller (CG). CT and CG send their signals (y_{CT} and y_{CG}) to a central controller (SDL). If a high temperature threshold (T_{max}) or a low flow rate threshold (G_{min}) is detected, then SDL sends a signal (y_{SDL}) which should activate an emergency shutdown (SCM). This safety device, commonly named SCRAM, consists in inserting (under gravity) control rods into the core which quickly stop the nuclear reaction by absorbing neutrons. The system variables are described in Sections 3.2 to 3.5.

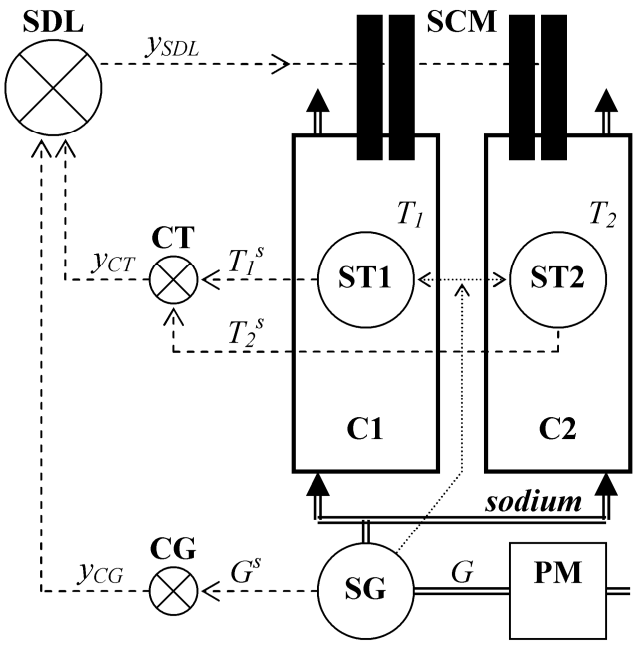

Figure 4. The Europa Fast Reactor

3.2 *Components State Variables*

The state of each of the eight system components is represented using a finite integer and constitutes one of the components of vector ***i(t)***, i.e. ***i(t)*** = ***(****SPM(t), SSG(t), SCG(t), SST1(t), SST2(t), SCT(t), SSDL(t), SSCM(t))*. In the following, and in accordance with the formalism presented in Section 2, each component of vector ***i(t)*** is modeled separately. The components state variables are then defined in Table 2.

The normal (full) operating modes of the components are represented by state variables equal to *1*. When a component state variable is equal to *0*, the corresponding failure mode is "dangerous," that is, it may directly yield an inability of the system to perform its safety function (i.e. inserting the control rods into the core). On the contrary, when a component state variable is equal to *2*, the corresponding failure mode is "safe," that is, it may directly yield a spurious activation of the safety function. Other values of component state variables (*3* or *4*) correspond, for example, to "degraded" modes of operation.

The state variables of the "mechanical" components, that is, the pump and the SCRAM, directly affect process variables as described in Section 3.3. On the other hand, the state variables of the controllers and transmitters directly determine data variables defined in Section 3.4. Finally, the effects of the "degraded" modes of operations are modeled using deviations variables defined in Section 3.5.

The transition rates between the possible states of each component are given in Table 3. Note that transition rates depend on time *t*, process variables, deviation variables, and states of other components. A deterministic (certain) transition is also assumed for the SCRAM activation (using a rate equal to $1/\Delta t$).

Table 2. Components state variables

System component	State variable	Possible value with description
pump (PM)	*SPM(t)*	*= 1* normal operation
		= 0 full failure
		= 3 degraded operation
flow rate transmitter (SG)	*SSG(t)*	*= 1* perfect results
		= 0 results locked to current value
		= 2 results locked to low value
flow rate controller (CG)	*SCG(t)*	*= 1* correct signals
		= 0 signals locked to "unsafe" value
		= 2 signals locked to "safe" value
temperature transmitters (STi) with *i = 1, 2*	*SSTi(t)*	*= 1* perfect results
		= 0 results locked to current value
		= 2 results locked to high value
		= 3 results subject to negative drifts
		= 4 results subject to positive drifts
temperature controller (CT)	*SCT(t)*	*= 1* correct signals
		= 0 signals locked to "unsafe" value
		= 2 signals locked to "safe" value
central controller (SDL)	*SSDL(t)*	*= 1* correct signals
		= 0 signals locked to "unsafe" value
		= 2 signals locked to "safe" value
SCRAM (SCM)	*SSCM(t)*	*= 1* normal operation
		= 0 full failure
		= 5 SCRAM activation

Table 3. Transition rates between components states

State variable	From state	To state	Transition rate* [s^{-1}]
SPM(t)	*1* or *3*	*0*	$1 \cdot 10^{-3} \cdot \exp(\delta_M(t) \cdot 5 \cdot 10^{-5})$
	1	*3*	$1 \cdot 10^{-2}$
SSG(t)	*1*	*0*	$2 \cdot 10^{-3}$
	1	*2*	$2 \cdot 10^{-4}$
SCG(t)	*1*	*0* or *2*	$1 \cdot 10^{-5}$
SST1(t)	*1*, *3* or *4*	*0*	$4 \cdot 10^{-4} \cdot (1+I_1(SST2(t)=0)) \cdot r(T_1(t))$
	1, *3* or *4*	*2*	$4 \cdot 10^{-5} \cdot (1+I_1(SST2(t)=2)) \cdot r(T_1(t))$
	1	*3* or *4*	$1.5 \cdot 10^{-2}$
SST2(t)	*1*, *3* or *4*	*0*	$4 \cdot 10^{-4} \cdot (1+I_1(SST1(t)=0)) \cdot r(T_2(t))$
	1, *3* or *4*	*2*	$4 \cdot 10^{-5} \cdot (1+I_1(SST1(t)=2)) \cdot r(T_2(t))$
	1	*3* or *4*	$1.5 \cdot 10^{-2}$
SCT(t)	*1*	*0* or *2*	$1 \cdot 10^{-5}$
SSDL(t)	*1*	*0* or *2*	$1 \cdot 10^{-6}$
SSCM(t)	*1*	*0*	$3.125 \cdot 10^{-8} \cdot t \cdot r((T_1(t)+T_2(t))/2)$
	1	*5*	$(1/\Delta t) \cdot I_1(y_{SDL}(t)=1)$

* $T_1(t)$ and $T_2(t)$ are process variables defined in Section 3.3, $\delta_M(t)$ is a deviation variable defined in Section 3.5, $I_1(.)$ and $r(.)$ are functions defined by Equations (12) and (13).

The following function is used to model the effect of the temperature process variables (T_1 and T_2) on transition rates (cf. Table 3):

$$r(T) = 6.17 \cdot 10^{-2} \cdot \exp(5.21 \cdot 10^{-3} \cdot T) \quad (12)$$

The following function is used to model dependencies with component states (e.g. between the temperature transmitters, cf. Table 3):

$I_1(A) = 1$ if assertion A is true, and 0 otherwise (13)

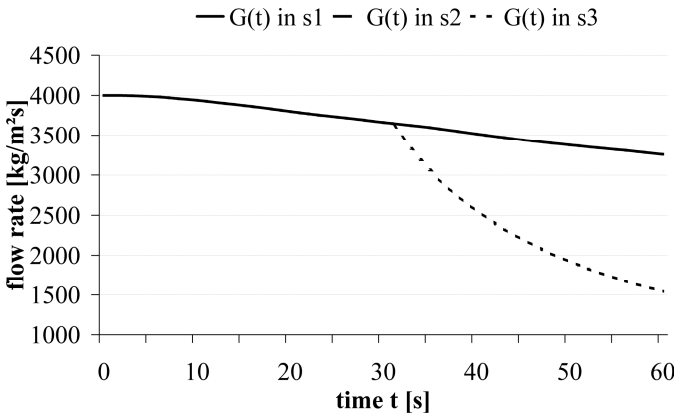

Figure 5. Flow rate evolution according to time t ($G(t)$), in scenarios s1, s2 (equivalent to s1), and s3, cf. Section 3.3

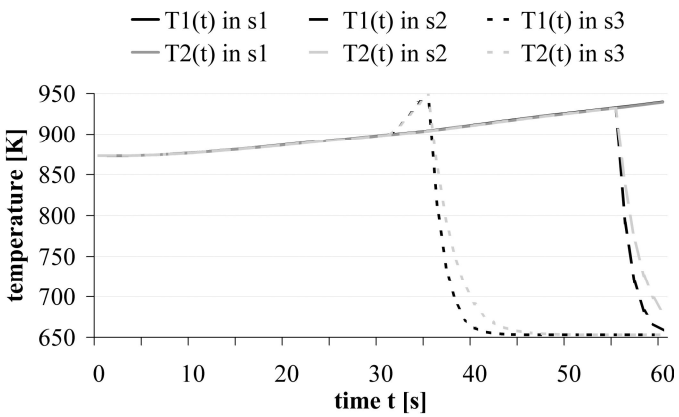

Figure 6. Temperature evolution according to time t ($T_1(t)$ and $T_2(t)$), in scenarios s1, s2, and s3, cf. Section 3.3

3.3 *Process Variables*

The thirteen process variables are $\boldsymbol{x(t)} = (\omega(t), G(t), T_{c,1}(t), T_{c,2}(t), T_1(t), T_2(t), P(t), C_1(t), C_2(t), C_3(t), C_4(t), C_5(t), C_6(t))$ and defined hereafter. Expressions of the derivatives are given by the following equations, with the initial conditions at time $t_0 = 0$. The parameters and their values are reported in Table 4.

Angular speed of the pump, denoted $\omega(t)$ [rad/s]:

$$\begin{cases} \frac{d}{dt}\varpi(t) = \frac{(C_M - \delta_M(t)) \cdot I_1(SPM(t) \neq 0) - K \cdot \varpi(t)}{I} \\ \omega(0) = \frac{C_M}{K} = 6000\ rad/s \end{cases} \quad (14)$$

where $\delta_M(t)$ is the pump torque deviation defined in Section 3.5, and $SPM(t)$ is the pump state variable defined in Section 3.2 (cf. Table 2).

Sodium linear momentum flow rate, denoted $G(t)$ [kg/m²s]:

$$\begin{cases} \frac{d}{dt}G(t) = \frac{\upsilon \cdot G(t)^2}{G(0)} + C_{nt2} \cdot (\omega(t)^2 - \omega(0)^2) - \upsilon \cdot G(0) \\ G(0) = 4000\ kg/m^2 s \end{cases} \quad (15)$$

Fuel temperature in channel i, denoted $T_{c,i}(t)$ [K], with $i = 1, 2$:

$$\begin{cases} \frac{d}{dt}T_{c,i}(t) = \frac{R \cdot w_i \cdot P(t) - (T_{c,i}(t) - T_e)}{\tau_i(T_{c,i}(t))} \\ T_{c,i}(0) = T_e + R \cdot w_i \cdot P(0) = \begin{cases} 1437K & if \quad i = 1 \\ 1773K & if \quad i = 2 \end{cases} \end{cases} \quad (16)$$

Table 4. Parameters

Parameter with value	Description
C_M = *60,000* N.m	nominal pump torque
K = *10* kg.m²/s	constant for pump friction
I = *10* kg.m²	pump moment of inertia
υ = $-5.00 \cdot 10^{-2}$ s^{-1}	constant for flow rate evolution
C_{nt2} = $5.56 \cdot 10^{-6}$ kg/m²	constant for flow rate evolution
R = $9.521 \cdot 10^{-7}$ K/W	thermal resistance
w_1 = *0.41175*	proportion of power generated by C1
w_2 = *0.58825*	proportion of power generated by C2
T_e = *653* K	sodium reactor inlet temperature
$\tau_1(T)$ = $1.1223+1.5215 \cdot 10^{-3} \cdot T - 1.0471 \cdot 10^{-6} \cdot T^2 + 2.7476 \cdot 10^{-10} \cdot T^3$	
$\tau_2(T)$ = $1.5714+2.1303 \cdot 10^{-3} \cdot T - 1.4661 \cdot 10^{-6} \cdot T^2 + 3.8470 \cdot 10^{-10} \cdot T^3$	
A_1 = *0.518867* m²	section of sodium passage in C1
A_2 = *0.741238* m²	section of sodium passage in C2
$C_R(T)$ = $1629 - 8.3290 \cdot 10^{-1} \cdot T$	sodium specific heat
γ_{SCM} = $4.40 \cdot 10^{-1}$ s^{-1}	reactivity induced by control rods
β_1 = $8.2100 \cdot 10^{-5}$	delayed neutron fraction
β_2 = $7.4480 \cdot 10^{-4}$	delayed neutron fraction
β_3 = $6.6150 \cdot 10^{-4}$	delayed neutron fraction
β_4 = $1.3277 \cdot 10^{-3}$	delayed neutron fraction
β_5 = $6.1480 \cdot 10^{-4}$	delayed neutron fraction
β_6 = $1.8940 \cdot 10^{-4}$	delayed neutron fraction
Γ = $3.98 \cdot 10^{-2}$ s	mean neutron production lifetime
γ_1 = $1.29 \cdot 10^{-2}$ s^{-1}	precursor decay constant
γ_2 = $3.11 \cdot 10^{-2}$ s^{-1}	precursor decay constant
γ_3 = $1.34 \cdot 10^{-1}$ s^{-1}	precursor decay constant
γ_4 = $3.31 \cdot 10^{-1}$ s^{-1}	precursor decay constant
γ_5 = *1.26* s^{-1}	precursor decay constant
γ_6 = *3.21* s^{-1}	precursor decay constant

Sodium temperature in channel *i*, denoted $T_i(t)$ [K], with $i = 1, 2$:

$$\begin{cases} \dfrac{d}{dt}T_i(t) = \dfrac{w_i \cdot P(t)}{2 \cdot A_i \cdot \tau_i\left(T_{c,i}(t)\right) \cdot C_R\left(T_i(t)\right) \cdot G(t)} \\ \quad -\left(\dfrac{1}{G(t)} \cdot \dfrac{d}{dt}G(t) + \dfrac{1}{\tau_i\left(T_{c,i}(t)\right)}\right) \cdot \left(T_i(t) - T_e\right) \\ T_i(0) = T_e + \dfrac{w_i \cdot P(0)}{2 \cdot A_i \cdot C_R\left(T_i(t)\right) \cdot G(0)} = 873\ K \end{cases} \quad (17)$$

Power generated by the core, denoted $P(t)$ [W]:

$$\begin{cases} \dfrac{d}{dt}P(t) = \left(-\gamma_{SCM} \cdot t \cdot \mathrm{I}_1\left(SSCM(t) = 5\right) - \sum_{i=1}^{6}\beta_i\right) \\ \quad \cdot \dfrac{P(t)}{\Gamma} + \sum_{i=1}^{6}\gamma_i \cdot C_i(t) \\ P(0) = 2000\ MW \end{cases} \quad (18)$$

where $SSCM(t)$ is the SCRAM state variable defined in Section 3.2 (cf. Table 2).

Precursor concentration, denoted $C_i(t)$ [W], with $i = 1, 2, 3, 4, 5, 6$:

$$\begin{cases} \dfrac{d}{dt}C_i(t) = -\gamma_i \cdot C_i(t) + \dfrac{\beta_i}{\Gamma} \cdot P(t) \\ C_i(0) = \dfrac{\beta_i}{\Gamma \cdot \gamma_i} \cdot P(0) \end{cases} \quad (19)$$

Note that the introduction of function $\mathrm{I}_1(A)$ allows the use of only one set of differential equations, which depend on components state variables as parameters. These equations also depend on deviation variables. Finally, Equations (14)-(19) are appropriate for the analyses presented in the present paper, but are not applicable to any other cases.

To illustrate the evolution of the flow rate $G(t)$ and temperatures $T_1(t)$ and $T_2(t)$, three scenarios are assumed and depicted in Figures 5 and 6:

- s1: $SPM(t) = 3$, and $SSCM(t) = 0$ for any time t;
- s2: $SPM(t) = 3$ for any time t, and $SSCM(t) = 1$ up to time $t = 53$ s, then $SSCM(t) = 5$;
- s3: $SPM(t)=3$ up to time $t = 30$ s, then $SPM(t)=0$, and $SSCM(t) = 1$ up to time $t = 33$ s, then $SSCM(t) = 5$.

In addition, the pump torque deviation $\delta_M(t)$ has been simulated according to Equation (26), using the same results for all these scenarios.

Table 5. Relationships between processing data $\alpha_i(t)$, and measurement results $T_i^s(t)$ and $G^s(t)$, with $i = 1, 2$

Measurement results	$\alpha_i(t)$
$T_i^s(t) = T_i(t)$ & $G^s(t) = G(t)$	$\alpha_i(t) = 0$
$T_i^s(t) < T_i(t)$ or $G^s(t) > G(t)$	$\alpha_i(t) < 0$
$T_i^s(t) > T_i(t)$ or $G^s(t) < G(t)$	$\alpha_i(t) > 0$

3.4 *Data Variables*

The ten data variables are $\mathbf{y(t)} = (G^s(t), T_1^s(t), T_2^s(t), y_{CG}(t), y_{CT}(t), y_{SDL}(t), \alpha_1(t), \alpha_2(t), T_1^c(t), T_2^c(t))$, and defined by the following equations. (cf. Table 2).

Measurement results, denoted $G^s(t)$ [kg/m²s], and $T_i^s(t)$ [K], with $i = 1, 2$:

$$\begin{aligned} G^s(t) &= G(t) \cdot \mathrm{I}_1\left(SSG(t) = 1\right) \\ &\quad + G^s(t - \Delta t) \cdot \mathrm{I}_1\left(SSG(t) = 0\right) + G_{\min} \cdot \mathrm{I}_1\left(SSG(t) = 2\right) \end{aligned} \quad (20)$$

$$\begin{aligned} T_i^s(t) &= \left(T_i(t) + T_i^c(t)\right) \cdot \mathrm{I}_1\left(SSTi(t) = 1, 3, or\ 4\right) \\ &\quad - \delta_{Di}(t) \cdot \mathrm{I}_1\left(SSTi(t) = 3\right) + \delta_{Di}(t) \cdot \mathrm{I}_1\left(SSTi(t) = 4\right) \\ &\quad + T_i^s(t - \Delta t) \cdot \mathrm{I}_1\left(SSTi(t) = 0\right) + T_{\max} \cdot \mathrm{I}_1\left(SSTi(t) = 2\right) \end{aligned} \quad (21)$$

where $\delta_{Di}(t)$ are drifts defined in Section 3.5. Note that data variables at time t depend on their values at time $t - \Delta t$ (cf. Sections 2).

Controller signals, denoted $y_{CG}(t)$, $y_{CT}(t)$, $y_{SDL}(t)$:

$$\begin{aligned} y_{CG}(t) &= \mathrm{I}_1\left(G^s(t) \le G_{\min}\right) \cdot \mathrm{I}_1\left(SCG(t) = 1\right) \\ &\quad + \mathrm{I}_1\left(SCG(t) = 2\right) \end{aligned} \quad (22)$$

$$\begin{aligned} y_{CT}(t) &= \mathrm{I}_1\left(T_1^s(t) \ge T_{\max}\ or\ T_2^s(t) \ge T_{\max}\right) \\ &\quad \cdot \mathrm{I}_1\left(SCT(t) = 1\right) + \mathrm{I}_1\left(SCT(t) = 2\right) \end{aligned} \quad (23)$$

$$\begin{aligned} y_{SDL}(t) &= \mathrm{I}_1\left(y_{CG}(t) = 1\ or\ y_{CT}(t) = 1\right) \cdot \mathrm{I}_1\left(SSDL(t) = 1\right) \\ &\quad + \mathrm{I}_1\left(SSDL(t) = 2\right) \end{aligned} \quad (24)$$

Processing data, denoted $\alpha_i(t)$ with $i = 1, 2$, are computed by the temperature transmitters according to other data variables (using communications between transmitters), in order to deduce characteristics on measurement results (cf. Table 5). These data are based on the derivatives of measurement results, compared to theoretical values (cf. Section 3.3):

$$\begin{aligned} \alpha_i(t) &= \frac{T_i^s(t + \Delta t) - T_i^s(t)}{\Delta t} \\ &\quad - \frac{w_i \cdot P(0)}{2 \cdot A_i \cdot \tau_i\left(T_{c,i}(0)\right) \cdot C_R\left(T_i^s(t)\right) \cdot G^s(t)} \\ &\quad + \left(\frac{G^s(t + \Delta t) - G^s(t)}{G^s(t) \cdot \Delta t} + \frac{1}{\tau_i\left(T_{c,i}(0)\right)}\right) \cdot \left(T_i^s(t) - T_e\right) \end{aligned} \quad (25)$$

According to $\alpha_i(t)$, parameters of drifts correction, denoted $T_i^c(t)$, with $i = 1, 2$, are then defined according to the rules given in Table 6, assuming $T_1(t) = T_2(t)$ before SCRAM activation (cf. Figure 6).

Table 6. Computation of $T_i^c(t)$ according to $\alpha_i(t)$, with $i = 1, 2$

Criteria* on $\alpha_i(t)$	Computation of $T_i^c(t)$
$\lvert\alpha_1(t)\rvert > \alpha_{ref}$ & $\lvert\alpha_2(t)\rvert < \alpha_{ref}$	$T_1^c(t) = T_2^s(t) - T_1^s(t)$ & $T_2^c(t) = T_2^s(t - \Delta t)$
$\lvert\alpha_1(t)\rvert < \alpha_{ref}$ & $\lvert\alpha_2(t)\rvert > \alpha_{ref}$	$T_2^c(t) = T_1^s(t) - T_2^s(t)$ & $T_1^c(t) = T_1^s(t - \Delta t)$
$\alpha_1(t) < -\alpha_{ref}$ & $\alpha_2(t) > \alpha_{ref}$ or $\alpha_1(t) > \alpha_{ref}$ & $\alpha_1(t) < -\alpha_{ref}$	$T_1^c(t) = ((T_2^s(t) - T_1^s(t))/2)$ & $T_2^c(t) = ((T_1^s(t) - T_2^s(t))/2)$
otherwise	$T_i^c(t) = T_i^s(t - \Delta t)$ with $i=1,2$

* For the basic case: $\alpha_{ref} = 1$

3.5 *Deviation Variables*

The three deviation variables are $\mathbf{e(t)} = (\delta_M(t), \delta_{D1}(t), \delta_{D2}(t))$ and are defined by the following equations.

The pump torque deviation, denoted $\delta_M(t)$ [N.m]:

$$\frac{d}{dt}\delta_M(t) = E_M(\mu,\sigma)\cdot \mathrm{I}_1(\delta_M(t) < C_M)\cdot \mathrm{I}_1(SPM(t) = 3) \quad (26)$$

with $E_M(\mu, \sigma)$ a random variable which follows a Log-Normal distribution of parameters $\mu = 5$, $\sigma = 1$.

The drifts, denoted $\delta_{Di}(t)$ [K], with $i = 1, 2$:

$$\frac{d}{dt}\delta_{Di}(t) = E_D(\delta_{Di}(t), T_i(t))\cdot \mathrm{I}_1(SSTi(t) = 3 \text{ or } 4) \quad (27)$$

with $E_D(\delta_{Di}(t), T_i(t))$ a random variable which follows an Exponential distribution of parameter $3\cdot 10^4/(T_i(t)\cdot\delta_{Di}(t) + 20)$, with $i = 1, 2$.

3.6 *Results*

The threshold values used for the analyses are $T_{max} = 923$ K and $G_{min} = 3345$ kg/m²s. At time $t_0 = 0$, all the system components are in the full operating modes (the components state variables are equal to *1*), except for the pump which is in the "degraded" mode of operation ($SPM(t_0) = 3$); the process variables are in the initial conditions defined in Section 3.3; the initial values of data variables are defined by Equations (20)-(25); and deviation variables are nil.

The system has been modeled using the formalism presented in Section 2, and its evolution has been simulated using CPN tools (Jensen *et al.* 2007), a Petri net software which provides all the characteristics required for the proposed modeling approach (including the color properties, the specification of random functions, and the definition of "meta-transition"). The scenarios of system evolution are then classified according to the temperatures in the reactor channels. If the SCRAM is activated while both T_1 and T_2 are lower than $T_{max} - 5 = 918$ K, then a "spurious trip" is assumed. On the other hand, if either T_1 or T_2 exceeds $T_{max} + 10 = 933$ K for more than *5* s, then a "hazardous event" is assumed. In the other cases, the system is "under control."

The analyses have been performed by Monte Carlo simulations (cf. Equation (10) and Section 2.3), and the results are reported in Table 7. To assess the effects of the "intelligent transmitter" features (the possibility to exchange information, to process data, and to offset drifts), a case without drift correction (i.e. $\alpha_{ref} = \infty$) is also presented. It is then shown that the use of such "intelligent transmitters" allows a greater percentage of "under control" cases, obtained by a reduction of the number of "spurious trips." However, a drawback of decreasing the probability of "spurious trips" is a slight increase of the percentage of "hazardous events." It is therefore deduced that adjustments of parameter α_{ref} should be used to balance reliability and safety.

Table 7. Percentage* of scenario realizations

Scenario	$\alpha_{ref} = \infty$	$\alpha_{ref} = 1.0$
under control	49.1	58.4
spurious trip	49.3	39.3
hazardous event	01.6	02.3

* Obtained through 1,000 Monte Carlo simulations trials.

4 REFERENCES

Aldemir, T. *et al.* (ed.) 1994. *Reliability and Safety Assessment of Dynamic Process Systems*. Berlin: Springer.

Aldemir, T. & Siu, N. (guest ed.) 1996. Special issue on reliability and safety analysis of dynamics process systems. *Reliability Engineering and System Safety* 52: 181-183.

Aldemir, T. *et al.* 2006. *Current State of Reliability Modeling Methodologies for Digital Systems and Their Acceptance Criteria for Nuclear Power Plant Assessments, NUREG/CR-6901*. Washington DC: US Nuclear Regulatory Commission.

Amendola, A. & Reina, G. 1984. *DYLAM-1: A Software Package for Event Sequence and Consequence Spectrum Methodology, EUR 9224 EN*. Luxembourg: Commission of European Communities.

Brissaud, F. *et al.* (submitted). Reliability analysis for new technology-based transmitters. Submitted for publication in *Reliability Engineering and System Safety*.

David, R. & Alla, H. 1994. Petri nets for modeling of dynamic systems: A survey. *Automatica* 30: 175-202.

Davis, M.H.A. 1993. *Markov models and optimization*. London: Chapman and Hall.

Devooght, J. & Smidts C. 1992a. Probabilistic Reactor Dynamics–I: The Theory of Continuous Event Trees. *Nuclear Science and Engineering* 111: 229-250.

Devooght, J. & Smidts C. 1992b. Probabilistic Reactor Dynamics–III: A Framework for Time-Dependent Interaction Between Operator and Reactor During a Transient Involving Human Error. *Nuclear Science and Engineering* 112: 101-113.

Dutuit, Y. *et al.* 1997. Dependability modelling and evaluation by using stochastic Petri nets: Application to two test cases. *Reliability Engineering and System Safety* 55: 117-124.

Jensen, K. *et al.* 2007. Coloured Petri Nets and CPN Tools for modelling and validation of concurrent systems. *International Journal on Software Tools for Technology Transfer* 9: 213-254.

Labeau, P.E. *et al.* 2000. Dynamic reliability: towards an integrated platform for probabilistic risk assessment. *Reliability Engineering and System Safety* 68: 219-254.

Siu, N. 1994. Risk assessment for dynamic systems: an overview. *Reliability Engineering and System Safety* 43: 43-73.

Smidts C. & Devooght J. 1992. Probabilistic Reactor Dynamics–II: A Monte Carlo Study of a Fast Reactor Transient. *Nuclear Science and Engineering* 111: 241-256.

Swaminathan S. & Smidts C. 2000. An application of the ESD framework to the probabilistic risk assessment of dynamic systems. *Proc. 5th Intern. Conf. Probabilistic Safety Assessment and Management, Osaka, 27 Nov.-1 Dec. 2000*.

US NRC 1975. *Reactor Safety Study (WASH-1400), NUREG-75/014*. Washington DC: US NRC.

Vernez, D. *et al.* 2003. Perspectives in the use of coloured Petri nets for risk analysis and accident modelling. *Safety Science* 41: 445-463.

Wider H.U. *et al.* 1989. *Comparative analysis of a hypothetical loss-of-flow accident in an irradiated LMFBR core using different computer models for a common benchmark problem, EUR 11925 EN*. Luxembourg: Commission of European Communities.